CLAIMS

What is claimed is:

1. A random number generator comprising:

a plurality of groups of independent flip-flops each of the groups having different configurations; and

each of the outputs of the plurality of groups of flip-flops being connected in an exclusive-or (XOR) network,

a latch connected to the output of the XOR network,

wherein a metastable output of at least one of flip-flop of the plurality of groups of flip-flops causes a random signal to be output by the XOR network for number generation.

2. The random number generator according to claim 1, wherein the groups of flip-flops are divided into at least three equally-sized groups.

3. The random number generator according to claim 2, wherein the first group of flip-flops comprises pairs of cross-connected NAND gates without any buffers inserted between the data and clock signals,

wherein the second group of flip-flops comprises at least one pair of cross-connected NAND gates with a data line of at least one NAND gate of the at least one pair of NAND gates being connected via a buffer; and

wherein the third group of flip-flops comprises at least one pair of cross-connected NAND gates having with a clock input of at least one NAND gate of each of the pairs of NAND gates being connected via a buffer.

4. The random number generator according to claim 2, wherein a first group of flip-flops comprises at least a pair of cross-connected NAND gates without any buffers between the cross connection,

wherein the second group of flip-flops comprises at least one pair of cross-connected NAND gates having a delay buffer connected to the output of an upper NAND gate of the pair of the NAND gates, and

wherein the third group of flip-flops (334) comprises at least one pair of cross-connected NAND gates havintg a delay buffer connected to the output of a lower NAND gate of each pair of the NAND gates.

5. The random number generator according to claim 2, wherein the first group of flip flops (394) comprises at least one pair of cross-connected NAND gates without any load added,

wherein the second group of flip flops comprises at least one pair of cross-connected NAND gates hqving a capacitive load connected to the data input of at least one pair of NAND gates, and

wherein the third group of flip flops comprises at least one pai4r of cross-connected NAND gates having a capacitive load connected to the clock input of at least one NAND gate of each of the at least one pair of NAND gates.

6. The random number generator according to claim 5, whereint he capacitive load comprises a mult-input gate.

7. The random number genera6tor according to claim 1, wherein the groups of flip flops have unequal numbers of flip flops in each group.

8. The random number generator according to claim 1, wherein each of the groups of flip flops have different delay values.

9. The random number generator according to claim 1, wherein a portion of the lfip flops are NAND gates, and the remainder are Boolean equivalents of NAND gates.

10. The random number generator according to claim 1, wherein the groups of flip flops are arranged into one of thirds or fifths.

11. A method for random number generation, comprising the steps of

(a) providing a plurality of groups of independent flip flops, each of the groups having different configurations; and

(b) connecting each of the outputs of the plurality of groups of flip flops in an exclusive-or (XOR) network,

(c) connecting a latch ot the output of the

XOR, so that a metastable output of at least one of flip flops cause a random signal to be output by the XOR network for receiopt by the latch for random number generation.

12. The method according to claim 11, wherein step (a) further comprises:

(i) arranging the groups of flip-flops into three equally-sized groups.

13. The method according to claim 12, wherein a first group comprises at least one pair of cross-connected NAND gtates without any buffers inserted between the data and clock signals,

wherein the second group comprises at least one pair of cross-connected NAND gates with a data line of at least one NAND gate of each of the pairs of NAND gates being connected via a buffer; and

wherein the third gorup comprises at least one pair of cross-connected NAND gates having with a clock input of at least one NAND gate of each of the pairs of NAND gates being connected via a buffer.

14. The method according to claim 12, wherein a first group comprises at least one pair of cross-connected NAND gates without any buffers between the cross connection,

the second group comprises at least one pair of cross-connected NAND gates having a delay buffer connected to the output of an upper NAND gate of each pair of the NAND gates, and

the third group comprises at least oen pair of cross-connected NAND gates having a delay buffer connected to the output of a lower NAND gate of each pair of the NAND gates.

15. The method according to claim 12, wherein a first group comprises at least one pair of cross-connected NAND gates without any load added,

wherein the second group comprises at least one pair of cross-connected NAND gates having a capacitive load connected to the data input of at least one NAND gate of each of the pairs of NAND gates, and

wherein the third group comprises at least one pair of cross-connected NAND gates having a capacitive load connected to the clock input of at least one NAND gate of each of the pairs of NAND gates.

16. The method according to claim 15, wherein the capacitive load provided comprises a multi-input gate.

17. The method according to claim 11, wherein step (a) further includes (i) arranging the groups of flip flops so that there are unequal numbers of flip flops in each group.

18. The method according to claim 11, wherein each of the gropus have different delay values.

19. The method according to claim 11, wherein a portion of the flip-flops provided in step (a) are NAND gates, and the remainder are Boolean equivalents of NAND gates.

20. The method according to claim 11, wherein the groups of flip flops are arranged into one of thirds or fifths.